

CLAIMS

1. A computer-readable medium storing a universal signature object for binding a digital signature to digital data, the universal signature object comprising:
 - at least one version of the digital data, wherein each version has a file format;
 - a digital signature of signature data, wherein the signature data is a function of the digital data; and
 - information concerning an application compatible with the file format of at least one of the versions.
2. The universal signature object of claim 1 wherein the file format of at least one version is a native file format of the digital data.
3. The universal signature object of claim 1 wherein the file format of at least one version is compatible with more than one application.
4. The universal signature object of claim 1 wherein the file format of at least one version is an alternate file format.
5. The universal signature object of claim 4 wherein the information concerning an application compatible with the file format of at least one of the versions includes information concerning an alternate application compatible with the alternate file format.
6. The universal signature object of claim 5 wherein the information concerning the alternate application includes an embedded executable file of the alternate application.

7. The universal signature object of claim 4 wherein the signature data is selected from the group comprising:

one of the versions of the digital data;

the universal signature object, prior to inclusion of the digital signature;

a hash of one of the versions of the digital data; and

a hash of the universal signature object, prior to inclusion of the digital signature.

8. The universal signature object of claim 4 wherein the digital signature is timestamped.

9. The universal signature object of claim 4 further comprising:

a public key, corresponding to a private key used to generate the digital signature.

10. The universal signature object of claim 4 further comprising an additional digital signature by an additional signatory of additional signature data, wherein the additional signature data is a function of the digital data.

11. The universal signature object of claim 10 wherein the additional signature data is selected from the group comprising:

one of the versions of the digital data;

the universal signature object, prior to inclusion of the additional digital signature;

a hash of one of the versions of the digital data; and

a hash of the universal signature object, prior to inclusion of the additional digital signature.

12. The universal signature object of claim 10 wherein the additional digital signature is timestamped.

13. The universal signature object of claim 1 wherein the signature data is selected from the group comprising:

one of the versions of the digital data;

the universal signature object, prior to inclusion of the digital signature;

a hash of one of the versions of the digital data; and

a hash of the universal signature object, prior to inclusion of the digital signature.

14. The universal signature object of claim 1 wherein the information concerning an application compatible with the file format of at least one of the versions includes information identifying the application compatible with the file format of at least one of the versions.

15. The universal signature object of claim 1 wherein the information concerning an application compatible with the file format of at least one of the versions includes an executable file of the application compatible with the file format of at least one of the versions.

16. The universal signature object of claim 1 wherein the digital signature is timestamped.

17. The universal signature object of claim 1 further comprising:

a public key, corresponding to a private key used to generate the digital signature.

18. The universal signature object of claim 1 further comprising an additional digital signature by an additional signatory of additional signature data, wherein the additional signature data is a function of the digital data.